



Broadcom Introduces VMware HyperArmor, Expanding Hypervisor Security and Protections for VMware Cloud Foundation

October 13, 2026

VMware HyperArmor offers unique, proactive zero day protection to VMware Cloud Foundation environments with no downtime, software upgrades, or in-guest agents

PALO ALTO, Calif., Oct. 13, 2026 (GLOBE NEWSWIRE) -- Broadcom Inc. (NASDAQ: AVGO), a global technology leader that designs, develops, and supplies semiconductor and infrastructure software solutions, today introduced VMware HyperArmor, a new software solution to help further protect the VMware ESX hypervisor component of VMware Cloud Foundation (VCF) against the exponential increase in cyber attack sophistication by closing exposure windows without disrupting the workloads that depend on the host.

"Frontier AI has changed the three V's of cybersecurity threats - the volume, velocity, and variety. When attacks come at machine speed, reactive detection and patching are no longer enough," said Paul Turner, chief product officer, VMware Cloud Foundation Division, Broadcom. "VMware HyperArmor takes a different approach by allowing only what is 'known good' to run on the host. With VMware vDefend already delivering virtual patching capabilities for the network layer of VMware Cloud Foundation, VMware HyperArmor now expands that protection around the hypervisor component itself."

As AI-accelerated threats grow in scale and sophistication, the threat surface now extends across every layer of the infrastructure stack including the hypervisor. Two problems account for most hypervisor attacks: stolen root credentials and unpatched vulnerabilities. VMware HyperArmor addresses both problems, with support for VMware ESX 8.x and later releases, as follows:

- **Virtual patching for VCF's ESX Component Host Environment.** HyperArmor delivers host-layer virtual patching to shield ESX by detecting and blocking attempted malicious actions within the host nodes before any vulnerabilities can be exploited. These host-level virtual patching capabilities complement the network-layer virtual patching available for VCF via VMware vDefend. Because virtual patching of ESX does not require host reboots or software upgrades to mitigate vulnerabilities, security teams will benefit from dramatically reduced risk windows and IT teams gain more operational flexibility to test and apply official patches on the schedule they prefer.
- **Positive Host Security Guardrails.** HyperArmor protects the host at the infrastructure layer, with no agents inside guest virtual machines (VMs). An ESX host runs a small, fixed set of processes. HyperArmor establishes a positive security baseline and automatically blocks any unauthorized executable or script. HyperArmor takes an inventory of scripts already on the host and allows them automatically, and administrators can approve new ones. The result is continuous monitoring and compliance enforcement with minimal performance overhead.
- **Hypervisor-level multi-factor authentication (MFA).** HyperArmor integrates MFA functionality directly into the ESX SSH login path. Logging in requires two steps: standard SSH credentials, followed by a secondary time-based one-time password challenge tied to a separately defined identity. Even if an attacker obtains the root password through phishing or credential leaks, they cannot reach the command line without that second factor.

"Attackers are using automation and AI to exploit infrastructure weaknesses faster than most organizations can patch, which means layered defense must extend all the way to the hypervisor as the foundation of the private cloud," said Stephen Elliot, Group Vice President, Software Development and IT Operations, IDC. "Technology leaders should prioritize preventive controls that help shrink exposure windows without disrupting production, and approaches that harden the virtualization layer natively rather than relying on external agents or post-incident detection."

Defense in Depth Across VMware Cloud Foundation

VMware HyperArmor works alongside the broader security capabilities in VMware Cloud Foundation to deliver an integrated and multi-layered approach. VMware Cloud Foundation is hardened out of the box with key capabilities that include centralized identity management, data-at-rest and data-in-transit encryption, and VMware vSphere live patching, which applies critical updates to the hypervisor without taking workloads down or placing hosts into full maintenance mode. VMware HyperArmor adds a proactive layer of protection for the hypervisor by blocking process execution exploits and credential theft. VMware vDefend delivers strong lateral security with micro-segmentation and advanced threat detection and prevention for VCF workloads, which uses deep traffic inspection to block emerging exploits and to deliver network-level virtual patching. VMware Avi Load Balancer provides web application and API protection (WAAP) for securing web and API traffic. Together, these layers give customers defense in depth across the infrastructure, network, and hypervisor.

Additional Resources

- Read "[Proactive Defense: Enhancing Hypervisor Security in the AI Era](#)," a blog from Prashanth Shenoy, VCF Division, Broadcom
- Learn more about [VMware HyperArmor](#)
- Learn more about [VMware Cloud Foundation](#)
- Follow VMware Cloud Foundation social channels on [LinkedIn](#), [X, formerly known as Twitter](#) and [YouTube](#)

About Broadcom

Broadcom Inc. (NASDAQ: AVGO) is a technology leader that designs, develops, and supplies semiconductors and infrastructure software for global organizations' complex, mission-critical needs. Broadcom combines long-term R&D investment with superb execution to deliver the best technology, at scale. Broadcom is a Delaware corporation headquartered in Palo Alto, CA. For more information, visit www.broadcom.com.

Broadcom, the pulse logo, and Connecting everything are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries. Other trademarks are the property of their respective owners.

Media Contact:

Roger T. Fortier

VMware Cloud Foundation Division, Broadcom

+1.408.348.1569

roger.fortier@broadcom.com